NASA Langley's

A Byzantine Fault-Tolerant and Self-Stabilizing Protocol

for distributed clock synchronization systems

NASA Langley researchers have developed and verified an approach to creating a self-stabilizing and Byzantine fault-tolerant protocol for distributed clock synchronization systems. Distributed computing systems are finding increasing usage in applications where individual nodes are operating independently, yet are linked into and serving the needs of a larger, more complex system. Clock synchronization is an example of a critical function for many distributed systems, and thus, fault tolerance and self-stabilization of clock synchronization are of key importance.

Benefits

- Self-stabilizes a distributed system of nodes from an arbitrary state
- Synchronizes nodes' clocks in the presence or absence of faults
- Operates independent of assumptions about the preexisting synchrony of the system and nodes
- Does not rely on a central clock or an externally generated pulse system
- Handles both transient and permanent faults
- Provides robustness to unpredictable faults in distributed systems
- Offers fast detection and recovery
- Deterministically converges in a short amount of time
- Offers low overhead and scalability
- Model has been verified

partnership opportunity

Applications

The technology offers wide-ranging market applications where self-stabilization can be used to design more robust distributed systems:

- Embedded systems
- Distributed process control
- Computer networks
- Internet and Internet applications
- Security and safety
- Automotive and other transport systems
- Telecommunication and other communication systems

The Technology

A distributed system is defined to be self-stabilizing when it can come from an arbitrary state and be in the presence of a bounded number of Byzantine faults, yet be guaranteed to reach a legitimate state in a finite amount of time and remain there as long as the number of faults are within a specific bound. (The legitimate state is a state where all good clocks in the system are synchronized within a given precision bound.)

The self-stabilization problem is both event-driven and time-driven. Most attempts on solving the problem to date have focused only on the event-driven aspect. The NASA protocol presented here merges both the time- and event-driven aspects in order to self-stabilize the system in a gradual yet timely manner. Furthermore, this protocol is based on a continual vigilance of the state of the system to maintain and guarantee its stabilized status. Finally, initialization and/or reintegration are regarded as inherent parts of this self-stabilizing protocol, and are not treated as special cases. A simplified model of the protocol has been model-checked and has proven to self-stabilize in the presence of one permanent Byzantine faulty node with arbitrarily malicious behavior.

For More Information

If your company is interested in licensing or joint development opportunities associated with this technology, or if you would like additional information on partnering with NASA, please contact:

The Technology Gateway

National Aeronautics and Space Administration

Langley Research Center
Mail Stop 218
Hampton, VA 23681
757.864.1178
LARC-DL-technologygateway@mail.nasa.gov
technologygateway.nasa.gov

www.nasa.gov

LAR-17391-1

Vol 1, Issue 17
NP-2008-04-77-LaRC